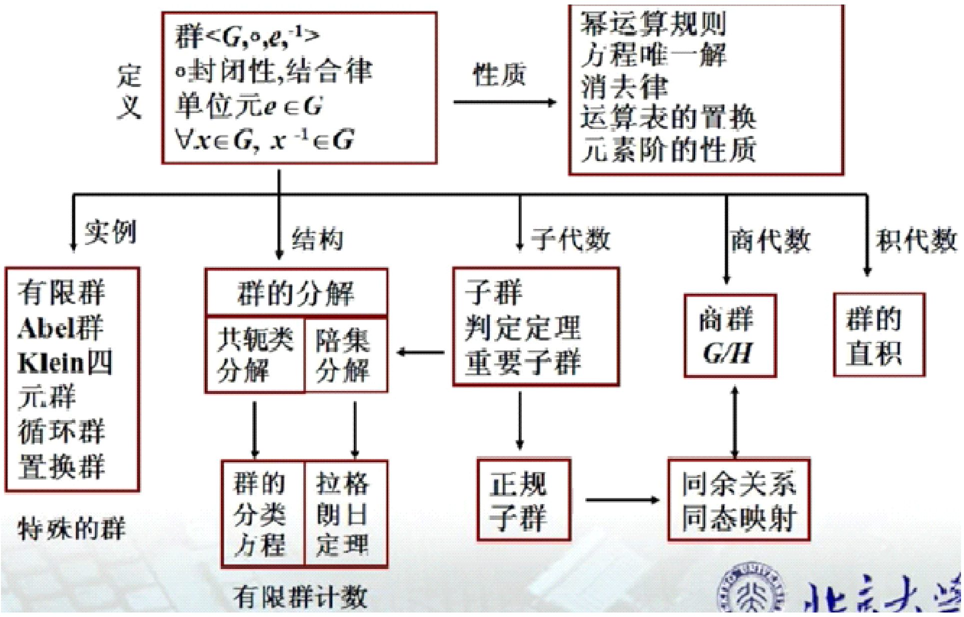
代数结构

2019年1月17日 0:10



一. 代数

1. 代数系统：非空集合S和S上k个一元或二元运算f组成的系统，简称代数
   1) 常记作<S,f1,f2,……,fk>
2. 半群：运算有结合性的代数
   1) 如d<Z,+><R,+><M_n(R),*><P(B),∪>
3. 格：两运算有交换律、结合律、幂等律和吸收率的代数
   1) 如<Z*,lcm,gcd><P(B),并集,交集>
4. 同态：同类型代数V1=<A,+>V2=<B,*>，f:A→B，且对任意x,y属于A，有f(x+y)=f(x)*f(y)，称f是V1到V2的同态映射，简称同态
   1) 若f是单射，称为单同态；如果是满射，称为满同态，并称V2是V1的同态像
   2) 若f是双射，称V1V2同构，记作全等于符号
   3) 同态时，有f(V1单位元e1)=V2单位元e2，f(V1零元θ1)=V2零元θ2，f(x^-1)=f(x)^-1

二. 群

1. 群：有满足以下性质的二元运算·的非空集合G，称为对·构成一个群
   1) 封闭性：∀ a∀ b，∃c=a·b（abc属于G）
   2) 结合性：∀ a∀ b∀ c，a·(b·c)=(a·b)·c
   3) 单位元：∀ a，∃e，e·a=a·e=a
   4) 逆元：∀ a，∃b，a·b=b·a=e
2. 群的性质
   1) 群的阶：群内元素量，阶无限时可称为无限群
   2) 元素的阶：通过与自己进行k次·运算后可变成单位元，则称该元素的阶为k
   3) 消去律：对存在逆元的元素a，a·b=a·c iff b=c

4) 一般不满足交换律，若满足则成为阿贝尔群，或加法群

3. 置换群：G上(goh)(x)=g(h(x))时(G,o)为置换群，阶为n时可记作Sym(n)
   1) 主观理解：1~n的一个全排列{an}交换顺序后得到新的全排列{bn}，称新排列{bn}为原排列{an}的n元置换，记作2行n列矩阵[1,…,n; a1,…,an]，列的顺序可换，视作同一种置换
   2) 连接运算：[1,…,n; a1,…,an][a1,…,an; b1,…,bn]=[1,…,n; b1,…,bn]满足结合律，不满足交换律
   3) 置换也可记作若干不相交循环的乘积

三. 域

1. 域：一个代数系统，有一个至少包含两个元素的非空集合F组成，在集合F上定义有两个二元运算：加法（用符号+ 表示）和乘法（用符号·表示），并满足下面条件，记为$<F,+,\cdot>$为域：
   a. F的元素关于加法‘+’成交换群，记其单位元为0（称为域的零元）；
   b. F关于乘法‘·’成交换群，记其单位元为1（称为域的单位元）；
   c. 乘法在加法上满足分配律，即对任意的$a,b,c\in F$，有$a\cdot(b+c)=ab+ac$，$(a+b)\cdot c=ac+bc$
2. 特殊的域：
   a. 若集合F只包含有限个元素，则称这个域F为有限域，也称为Galois域；有限域中的元素个数也称为该有限域的阶。
   b. 若有一任意的素数P和正整数$n\in Z^+$，存在P^n阶有限域，这个有限域记为GF(P^n)，当n=1时，有限域GF(P)称为**素域**。